arXiv:math-ph/9907014v1 16 Jul 1999

On cyclically shifted strings

K. Bärwinkel, H.-J. Schmidt [1], J. Schnack

Universität Osnabrück, Fachbereich Physik
Barbarastr. 7, 49069 Osnabrück, Germany

Abstract

If a string is cyclically shifted it will re–appear after a certain number of shifts, which will be called its *order*. We solve the problem of how many strings exist with a given order. This problem arises in the context of quantum mechanics of spin systems.

1 Introduction and definitions

Let $\mathcal{S}(A,N)$ denote the set of strings $a = \langle a_1, \ldots, a_N\rangle$ of natural numbers $a_n \in \{0, \ldots, A-1\}$. There are exactly A^N such strings. For any $a \in \mathcal{S}(A,N)$ let $\Sigma(a) \stackrel{\text{def}}{=} \sum_{n=0}^{N} a_n$ and $T(a) \stackrel{\text{def}}{=} \langle a_N, a_1, a_2, \ldots, a_{N-1}\rangle$. T is the cyclic shift operator. If T^n denotes the nth power of T, $n \in \mathbb{N}$, it follows that $T^N = T^0 = \mathbf{1}_{\mathcal{S}(A,N)}$.
We consider two equivalence relations on $\mathcal{S}(A,N)$. For $a, b \in \mathcal{S}(A,N)$ we define

$$a \sim b \Leftrightarrow \Sigma(a) = \Sigma(b) \tag{1}$$

and

$$a \approx b \Leftrightarrow a = T^n(b) \text{ for some } n \in \mathbb{N}. \tag{2}$$

Obviously, $a \approx b$ implies $a \sim b$ since the sum of the numbers in a string is invariant under permutations.
The aim of this article is to analyze the structure of the equivalence classes of strings with respect to $\sim$ and $\approx$. The main question will be: How many $\approx$-equivalence classes of a given size exist? Or: How many $\approx$-equivalence classes of a given size exist which are contained in a certain $\sim$-equivalence class? This problem can, of course, be solved in a straight-forward manner for any given A and N, either by hand or by means of a simple computer program. We are rather seeking explicit

[1] corresponding author: hschmidt@uos.de,
http://www.physik.uni-osnabrueck.de/makrosysteme/

formulae which answer the above questions.
The problem arises in the context of quantum mechanics of spin rings with a cyclically symmetric coupling between the N individual spins. Any individual spin can assume A different states and the total system can assume A^N different states. More precisely: The total Hilbert space of the problem possesses an orthonormal basis of product states parametrized by the set $\mathcal{S}(A,N)$. According to the symmetries of the problem it is possible to split the total Hilbert space into a sum of orthogonal subspaces which are invariant under the Hamiltonian of the problem. These subspaces are closely connected to the equivalence classes of strings defined above. For more details see [1–3].

2 Strings with constant sum

For any $a \in \mathcal{S}(A,N)$ we denote the equivalence class of strings having the same sum by

$$[a]_\sim \stackrel{\text{def}}{=} \mathcal{S}(A,N,M) \quad \text{where } M \stackrel{\text{def}}{=} \Sigma(a). \tag{3}$$

Obviously, $\mathcal{S}(A,N)$ is a disjoint union

$$\mathcal{S}(A,N) = \bigcup_{M=0\ldots N(A-1)} \mathcal{S}(A,N,M) \tag{4}$$

and the total number of strings satisfies

$$|\mathcal{S}(A,N)| = A^N = \sum_{M=0\ldots N(A-1)} |\mathcal{S}(A,N,M)| \,. \tag{5}$$

The problem of determining the number of strings with a constant sum $|\mathcal{S}(A,N,M)|$ is equivalent to the problem of calculating the probability distribution of the sum of N independent, finite, uniformly distributed random variables. An example would be the probability of scoring the sum M in a throw with N dice with A faces. Geometrically, this is the problem of how many lattice points are met if you cut a hypercube containing A^N lattice points perpendicular to its main diagonal.
The solution to this problem is known since long and traces back to Abraham de MOIVRE[4]:

$$|\mathcal{S}(A,N,M)| = \sum_{n=0}^{\lfloor \frac{M}{A} \rfloor} (-1)^n \binom{N}{n} \binom{N-1+M-nA}{N-1}, \tag{6}$$

where $\lfloor x \rfloor$ denotes the largest integer $\leq x$. The proof is straight-forward using the generating function (see e. g. [5])

$$\left(\sum_{a=0}^{A-1} z^a \right)^N = \sum_{m=0}^{N(A-1)} |\mathcal{S}(A,N,m)| \, z^m. \tag{7}$$

3 Cycles of strings

We will call the equivalence classes $\mathbf{a} = [a]_{\approx}, \quad a \in \mathcal{S}(A, N)$ of strings which are connected by cyclic shifts "cycles". The different sets of cycles will be denoted by

$$\mathcal{C}(A, N) \stackrel{\text{def}}{=} \mathcal{S}(A, N)/\approx, \quad \mathcal{C}(A, N, M) \stackrel{\text{def}}{=} \mathcal{S}(A, N, M)/\approx . \tag{8}$$

This notation appears natural since cycles are the orbits of the cyclic group

$$G \stackrel{\text{def}}{=} \{T^n : n = 0, \ldots, N-1\} \cong \mathbb{Z}_N \tag{9}$$

operating on strings in the way defined above. Hence cycles can at most contain N strings. The number of strings contained in a cycle will be called its "order". "Proper cycles" are defined as those of maximal order N, "epicycles" are cycles of order less than N. Special epicycles are those containing exactly one constant string $a = \langle i, i, \ldots, i \rangle, i \in \{0, \ldots, A-1\}$. These will be of order one and are called "monocycles". Obviously, there are exactly A monocycles.
Generally, the orbit of a group G generated by the operation on some element a will be isomorphic to the quotient set G/G_a, where G_a is defined as the subgroup of all transformations leaving a fixed. In our case G_a will be isomorphic to $\mathbb{Z}_k$ where k is a divisor of N and $\mathbf{a}$ will be of order $n = \frac{N}{k}$. The case $k = 1$ corresponds to proper cycles, whereas the case $k = N$ yields monocycles.
To put it differently: If a string $a \in \mathcal{S}(A, N)$ consists of k copies of a substring $b \in \mathcal{S}(A, n)$, $kn = N$, it will generate an epicycle $\mathbf{a} = [a]_{\approx}$ containing at most n strings. $\mathbf{a}$ contains exactly n strings iff b itself generates a proper cycle $\mathbf{b} \in \mathcal{C}(A, n)$. Conversely, any epicycle $\mathbf{a}$ of order n consists of strings which are k copies of substrings b belonging to proper cycles $\mathbf{b}$. Moreover, if $\mathbf{a} \in \mathcal{C}(A, N, M)$ is of order n the corresponding proper cycle $\mathbf{b}$ will satisfy $\mathbf{b} \in \mathcal{C}(A, n, m)$ with $M = km$. Thus we obtain the following

Lemma 1 *(1) The order n of any cycle $\mathbf{a} \in \mathcal{C}(A, N, M)$ is a divisor of N.*

(2) Moreover, in this case $m \stackrel{\text{def}}{=} \frac{Mn}{N}$ will be an integer.

Hence the order of cycles will always belong to the following set:

Definition 1 $\mathcal{D}(A, N, M) \stackrel{\text{def}}{=} \{n \in \mathbb{N} : n|N$ *and* $N|Mn\}$.

In passing we note that if N is a prime number, then there will be only proper cycles and exactly A monocycles, as mentioned above, hence N will divide $A^N - A$, which is essentially FERMAT's theorem of 1640.

Definition 2 *Let $\mathcal{N}(A, N, M, n)$ denote the number of cycles $\mathbf{a} \in \mathcal{C}(A, N, M)$ of*

order n and $\mathcal{M}(A,N,M,n)$ the number of strings belonging to these cycles:

$$\mathcal{M}(A,N,M,n) \stackrel{\text{def}}{=} \mathcal{N}(A,N,M,n)n. \tag{10}$$

According to the preceding discussion the following holds:

Lemma 2

$$|\mathcal{S}(A,N,M)| = \sum_{n\in\mathcal{D}(A,N,M)} \mathcal{M}(A,N,M,n), \tag{11}$$

$$\mathcal{N}(A,N,M,n) = \begin{cases} \mathcal{N}(A,n,\frac{Mn}{N},n) & : \quad \textit{if } n \in \mathcal{D}(A,N,M) \\ 0 & : \quad \textit{else} \end{cases} . \tag{12}$$

Together with (6) this yields a recursion relation for $\mathcal{M}(A,N,M,n)$. It is, however, possible to obtain an explicit formula, which will be shown in the next section.

4 Explicit formula for $\mathcal{M}(A,N,M,n)$

Let us consider for example $N = 12$. Then (11) yields the following equations, where redundant arguments will be suppressed:

$$\begin{aligned} |\mathcal{S}(A,12,M)| &\stackrel{\text{def}}{=} S_{12} \\ &= \mathcal{M}(A,12,M,12) + \mathcal{M}(A,6,M/2,6) + \mathcal{M}(A,4,M/3,4) \\ &\quad + \mathcal{M}(A,3,M/4,3) + \mathcal{M}(A,2,M/6,2) + \mathcal{M}(A,1,M/12,1) \\ &\stackrel{\text{def}}{=} M_{12} + M_6 + M_4 + M_3 + M_2 + M_1 \\ &= M_{12} + (S_6 - M_3 - M_2 - M_1) + (S_4 - M_2 - M_1) \\ &\quad + (S_3 - M_1) + (S_2 - M_1) + S_1 \\ &= M_{12} + (S_6 - (S_3 - S_1) - (S_2 - S_1) - S_1) + \\ &\quad (S_4 - (S_2 - S1) - S_1) + (S_3 - S_1) + (S_2 - S_1) + S_1 \\ &\Rightarrow \\ M_{12} &= S_{12} - S_6 - S_4 + (1-1)S_3 + (1+1-1)S_2 + \\ &\quad (-1-1+1-1+1+1+1-1)S_1 \,. \end{aligned} \tag{13}$$

We see how each S_n will enter in different ways into the expression for M_{12} according to different "divisor chains" $n|\ldots|N$. Here by a "divisor chain" we understand a finite sequence of numbers each of which is a divisor of the next one. In the example, there are "odd" divisor chains $6|12$, $4|12$, $3|12$, $2|12$, $1|3|6|12$, $1|2|6|12$, $1|2|4|12$ (with an odd number of strokes $|$), and "even" divisor chains $3|6|12$, $2|6|12$, $2|4|12$, $1|6|12$, $1|4|12$, $1|3|12$ and $1|2|12$. Each even divisor chain $n|\ldots|12$ yields

a term $+S_n$, each odd one a term $-S_n$ in the expression for M_{12}.

Generalizing this example, we conclude that

$$\mathcal{M}(A,N,M,N) = \sum_{n \in \mathcal{D}(A,N,M)} \Delta_{n,N} \cdot \left| \mathcal{S}(A,n,\frac{Mn}{N}) \right| \tag{14}$$

where $\Delta_{n,N}$ is defined as the number of even divisor chains $n|\ldots|N$ minus the number of odd divisor chains $n|\ldots|N$.
Thus the problem is reduced to the task of finding an explicit formula for $\Delta_{n,N}$. Obviously, $\Delta_{n,N} = \Delta_{1,N/n} \stackrel{\text{def}}{=} \Delta_{N/n}$ if $n|N$. Let $K = N/n$. Each divisor chain $k_0 = 1|k_1|k_2|\ldots|k_\mu = K$ corresponds in a $1:1$ manner to a factorization of K of the form $K = \frac{k_1}{1} \cdot \frac{k_2}{k_1} \cdots \frac{k_\mu}{k_{\mu-1}} \stackrel{\text{def}}{=} K_1 \cdot K_2 \cdot \ldots \cdot K_\mu$. Of course, permutations of different factors count as different factorizations since they give rise to different divisor chains. Even (resp. odd) divisor chains correspond to even (resp. odd) μ.

Lemma 3 *If K is a product of ν different primes, $K = p_1 p_2 \ldots p_\nu$, then $\Delta_K = (-1)^\nu$.*

Proof: We proceed by induction. If K is prime, i. e. $\nu = 1$, there is only one odd (trivial) factorization $K = K_1$ and $\Delta_K = -1$.
Next we assume the formula to be valid for K and are going to prove it for $K' = K \cdot p_{\nu+1}$, where $p_{\nu+1}$ is a prime different from $p_1, \ldots, p_\nu$. Let $K = K_1 \cdots K_\mu$ be an arbitrary factorization of K. There are two processes to obtain from this a factorization of K': Multiplication of one of the μ factors by $p_{\nu+1}$, which does not alter the even/odd character of the factorization. The other process is insertion of $p_{\nu+1}$ into one of $\mu+1$ places. This yields a factorization of length $\mu+1$ and hence changes the even/odd character. Obviously, every factorization of K' will be obtained by exactly one of these two procedures. Denote by $O(K)$ the number of odd factorizations of K and by $E(K)$ the number of even ones. Then the preceding argument shows that

$$E(K') = \mu E(K) + (\mu+1) O(K), \tag{15}$$

and

$$O(K') = \mu O(K) + (\mu+1) E(K). \tag{16}$$

Subtraction yields $E(K') - O(K') = O(K) - E(K)$, hence $\Delta_{K'} = -\Delta_K = (-1)^{\nu+1}$. ■

Lemma 4 *If in the prime factorization of K at least one prime occurs twice or more, then $\Delta_K = 0$.*

Proof: Let $K' = K \cdot p_{\nu+1}$ as in the preceding proof, but $p_{\nu+1}|K$. If $K' = K'_1 \cdot K'_1 \cdots K'_{\mu'}$ is any factorization of K', it may be obtained from factorizations of

K by different processes of multiplication by or insertion of $p_{\nu+1}$. (For example, $12 = 3 \cdot 2 \cdot 2$ may be obtained from $6 = 3 \cdot 2$ by insertion at two different places.) In order to make the process unique we make the convention to delete the leftmost occurrence of $p_{\nu+1}$ in $K' = K'_1 \cdot K'_2 \cdots K'_{\mu'}$ thereby arriving at a factorization of K. Vice versa, this means that we will only multiply or insert $p_{\nu+1}$ left from K_λ (including K_λ in the case of multiplication), if K_λ is the first factor with $p_{\nu+1}|K_\lambda$. Hence $p_{\nu+1}$ can be multiplied with λ factors and inserted at λ places whence

$$E(K') = \lambda E(K) + \lambda O(K), \tag{17}$$

and

$$O(K') = \lambda O(K) + \lambda E(K). \tag{18}$$

Subtraction yields $E(K') = O(K')$ and thus $\Delta_{K'} = 0$. ■

In order to formulate our main result we define

$$q(\nu) \stackrel{\text{def}}{=} \begin{cases} (-1)^m & : \quad \text{if } \nu \text{ is a product of } m \text{ different primes,} \\ 0 & : \quad \text{else} \end{cases} . \tag{19}$$

Summarizing, we have proven the following

Theorem 1

$$\mathcal{M}(A,N,M,N) = \sum_{n \in \mathcal{D}(A,N,M)} q(\frac{N}{n}) \sum_{\nu=0}^{\lfloor \frac{Mn}{NA} \rfloor} (-1)^\nu \binom{n}{\nu} \binom{n-1+\frac{Mn}{N}-\nu A}{n-1}, \tag{20}$$

$$\mathcal{M}(A,N,M,n) = \begin{cases} \mathcal{M}(A,n,\frac{Mn}{N},n) & : \quad \textit{if } n \in \mathcal{D}(A,N,M) \\ 0 & : \quad \textit{else} \end{cases} \tag{21}$$

Let $\mathcal{M}(A,n)$ denote the number of strings belonging to cycles of order n, irrespective of M. This number does not depend on the total length N of the strings. By an analogous reasoning as above we may conclude

Theorem 2

$$\mathcal{M}(A,n) = \sum_{k|n} q(\frac{n}{k}) A^k. \tag{22}$$

From this the number of cycles is obtained by division by n. Note that $n|\mathcal{M}(A,n)$, hence (22) generalizes FERMAT's original result to the case where n need not be

Order n	Number of cycles of order n
1	5
2	10
3	40
4	150
6	2580
12	20343700

Table 1
Number of cycles of order n for $N = 12$ and $A = 5$.

prime.
We close the article by giving a numerical example for $N = 12$ and $A = 5$ in table 1.

References

[1] D. Kouzoudis, *Heisenberg* $s = \frac{1}{2}$ *ring consisting of a prime number of atoms*, J. Magn. Magn. Mater. **173** (1997) 259

[2] D. Kouzoudis, *Exact analytical partition function and energy levels for a Heisenberg ring of* $N = 6$ *spin 1/2 sites*, J. Magn. Magn. Mater. **189** (1998) 366

[3] K. Bärwinkel, H.-J. Schmidt, J. Schnack, *Structure and relevant dimension of the Heisenberg model and applications to spin rings*, submitted to J. Magn. Magn. Mater. (1999)

[4] A. de Moivre, *Miscellanea Analytica*, (1730), 191-197

[5] W. Feller, *An introduction to probability theory and its applications*, Vol. 1, 3. ed., John Wiley & Sons, New York (1968) chapter XI.7, problem 18